자동차 안전 무결성 수준(ASIL)에 대한 가이드

자동차 기술의 새로운 혁명은 지평선에 있는 것이 아니라 이미 왔습니다. 전기 자동차의 급속한 확산에서 자율 주행 자동차에 이르기까지 자동차는 기계 시스템 시대에서 빠르게 발전했습니다. 이러한 발전은 다양한 이유로 흥미롭고 환영받지만, 와이퍼에서 마이크로칩, 내장 카메라에 이르기까지 모든 것을 개발하는 개발자에게는 점점 더 많은 과제와 고려 사항이 따릅니다. 운전자가 A 지점에서 B 지점으로 이동하는 것을 더 쉽고 재미있게 만드는 시스템에 점점 더 의존하게 되면서, 이러한 시스템이 안전하고 신뢰할 수 있다는 확신도 필요합니다.

이 새로운 자동차 현실에서 안전 지침을 준수하는 것은 그 어느 때보다 중요합니다. 개발자와 제조업체가 ISO 26262를 준수하기 위해 노력하면서 자동차 안전 무결성 수준(ASIL)을 이해하여 어떤 수준의 엄격성을 적용해야 하는지 알아야 합니다.

ASIL이란 무엇인가요?

ASIL은 Automotive Safety Integrity Level의 약자로, 도로 차량의 기능적 안전을 위한 위험 분류 시스템입니다. ASIL은 ISO 26262 표준 9부에 의해 정의되며 IEC 61508에 게시된 Safety Integrity Level(SIL) 지침에서 수정되었습니다.

ISO 26262 준수는 필수는 아니지만 업계의 최첨단 관행이며 ASIL은 표준의 핵심 부분입니다. ASIL은 제품이 실패할 경우 사람에게 해를 끼칠 위험에 따라 제품을 개발하는 프로세스가 얼마나 엄격해야 하는지 결정합니다. 다양한 요인에 따라 각 구성 요소, 모듈 또는 시스템에 대한 전체 안전 평가를 수행함으로써 팀은 실패 시 위험과 결과에 대한 합리적인 기대에 도달하고 위험을 줄이기 위한 완화 노력을 구현할 수 있습니다.

ASIL은 전체 위험 분석 및 위험 평가 또는 HARA를 거친 후 결정됩니다. 엔지니어 또는 개발자는 각 구성 요소 또는 시스템을 해당 구성 요소 또는 시스템의 잠재적 고장으로 인해 발생하는 위험과 위험을 고려하여 평가합니다. 시스템이 고장날 가능성은 얼마나 됩니까? 고장이 발생하면 어떻게 됩니까? 운전자가 부상 없이 고장을 보상하거나 관리할 수 있습니까? 고장이 발생할 경우 부상이 발생할 가능성이 있습니까? 그렇다면 부상은 얼마나 심각할까요? 위험 분석 및 위험 평가가 완료되면 팀은 ASIL을 할당할 수 있습니다.

관련 기사: IEC 61508 개요: 산업 제조의 기능 안전을 위한 완벽한 가이드

ASIL에는 어떤 것들이 있나요?

ASIL은 위험을 A에서 D까지 4단계로 분류하며, 위험하지 않은 시스템이나 구성 요소에는 5단계가 추가됩니다. ASIL D는 가장 높은 위험 수준을 나타내고, ASIL A는 가장 낮은 위험 수준을 나타냅니다. 추가 단계인 QM은 품질 관리를 의미하며 표준 품질 관리 준수만 필요한 위험하지 않은 품목을 나타냅니다.

일반적으로 잠금 방지 브레이크나 에어백과 같은 시스템은 고장과 관련된 위험이 가장 높기 때문에 ASIL D 분류가 필요합니다. 스펙트럼의 다른 쪽 끝에서 후방등과 같은 시스템은 ASIL A 분류만 필요합니다. 후방등과 관련된 안전 구성 요소가 확실히 있지만 대부분 운전자는 이러한 위험을 완화할 수 있으며 부상의 잠재적 심각성은 일반적으로 높지 않습니다.

ASIL을 결정하는 요소는 무엇입니까?

ASIL을 결정하기 위해 개발자와 엔지니어는 다음 세 가지 요소를 고려합니다.

- **심각도** (위험한 사건으로 인한 부상의 잠재적 심각도)
- **노출** (잠재적으로 부상을 일으킬 수 있는 조건의 빈도)
- **제어 가능성** (운전자가 부상을 예방하기 위해 행동할 수 있는 가능성)

세 가지 요소 각각 내에는 숫자로 표현된 추가 수준이 있습니다.

심각성

S0: 부상 없음

S1: 경미한 부상에서 중간 정도의 부상

S2: 심각한 부상에서 생명을 위협하는 부상(생존 가능성 높음)

S3: 생명을 위협하는(생존 불확실) 부상에서 치명적인 부상까지

노출

E0: 믿을 수 없을 정도로 가능성이 낮음

E1: 매우 낮은 확률

E2: 낮은 확률

E3: 중간 확률

E4: 높은 확률(대부분의 작동 조건에서 부상이 발생할 수 있음)

제어 가능성

C0: 일반적으로 제어 가능

C1: 간단하게 제어 가능

C2: 일반적으로 제어 가능(대부분 운전자가 부상을 예방하기 위해 행동할 수 있음)

C3: 제어하기 어렵거나 제어할 수 없음

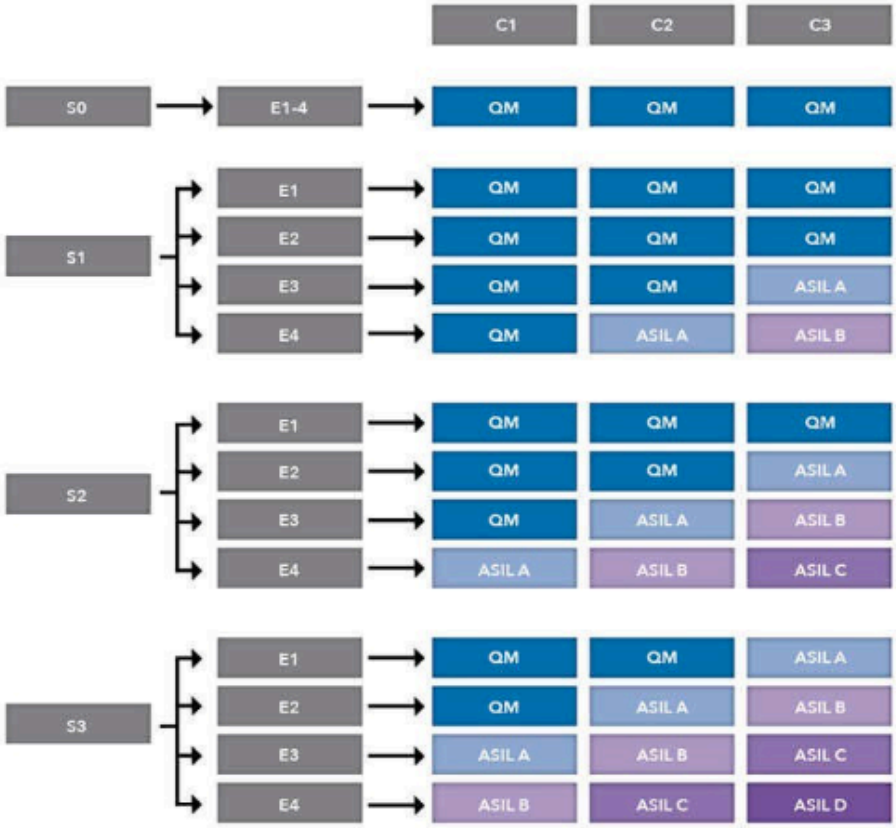
관련 기사: 자동차 개발에 대한 ISO 26262의 영향

ASIL은 어떻게 선택하나요?

ASIL을 결정하기 위해 개발팀은 각 시스템, 모듈 또는 구성 요소를 전체 위험 분석 및 위험 평가(HARA)에 통과시켜야 합니다. 이 평가의 목적은 위험이나 실패로 이어질 수 있는 모든 오작동을 식별하고 해당 실패와 관련된 위험을 평가하는 것입니다. 모든 제품에 대해 ISO 26262 준수를 목표로 하는 모든 제조업체는 HARA를 수행하고 ASIL을 지정해야 합니다.

HARA 동안 팀은 위의 차트에서 확립된 심각도, 노출 및 제어 가능성 수준을 할당합니다. 이러한 수준이 해당 범주 내에서 확립되면 팀은 아래 차트를 사용하여 ASIL에 도달할 수 있습니다.

참고 사항: 이 가이드는 ASIL을 일반적으로 식별하는 데 도움이 될 수 있지만 공식적인 ASIL 결정 기준으로 사용되어서는 안 됩니다.



더 자세히 알아볼 준비가 되셨나요?

저희 전문가 팀은 모든 질문에 답하고 귀하의 지속적인 성공을 위해 어떻게 도울 수 있는지 알아보기 위해 여기 있습니다. 무료 30일 체험판으로 시작하거나 데모를 예약하세요!

무료 30일 체험

데모 예약하기

ASIL 분류의 예로는 어떤 것들이 있나요?

다양한 ASIL 분류에는 어느 정도 주관성이 있지만, 일부 시스템과 구성 요소는 상당히 일관된 분류를 가지고 있습니다. 몇 가지 예는 다음과 같습니다.

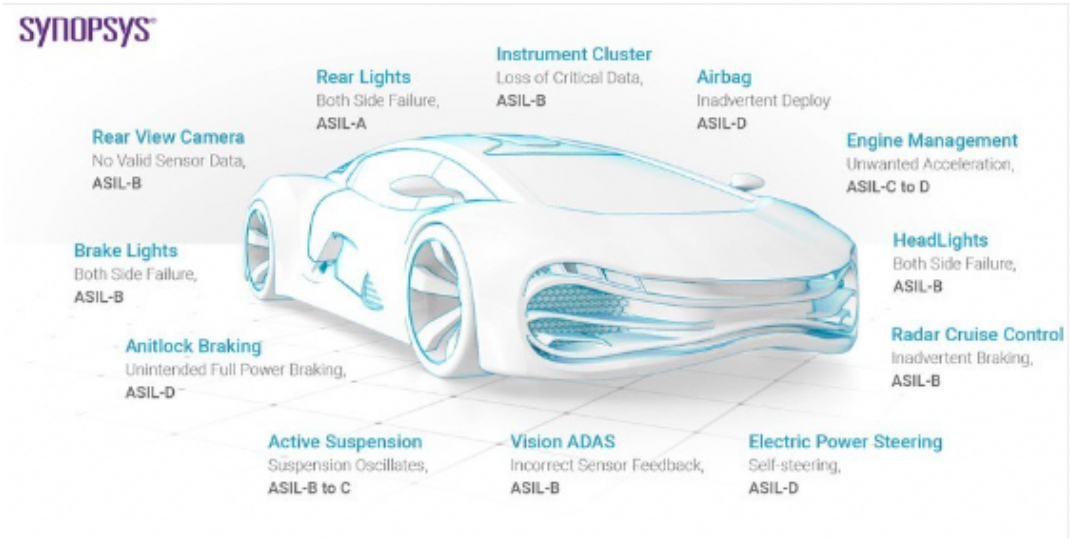
ASIL D: 에어백, ABS, 전동 파워 스티어링

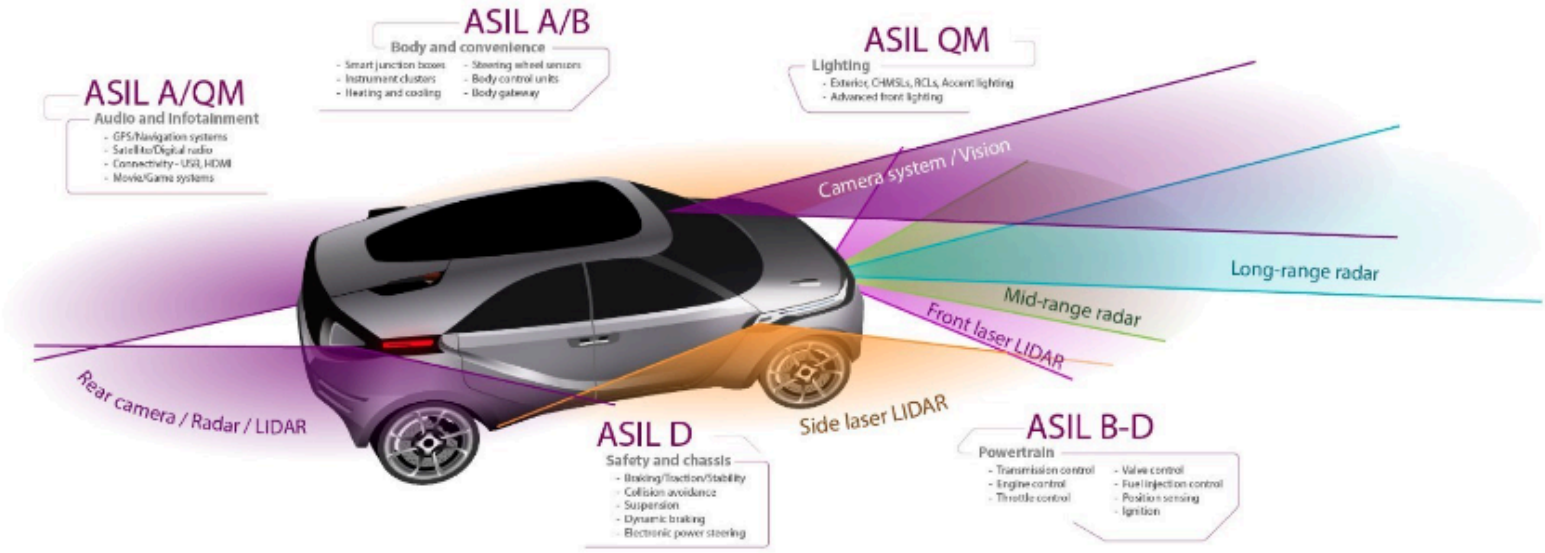
ASIL C: 적응형 크루즈 컨트롤, 배터리 관리, 서스펜션

ASIL B: 브레이크 라이트, 후방 카메라, 계기판

ASIL A: 후방등, 난방 및 냉각, 차체 제어 장치

QM: GPS/내비게이션 시스템, 위성/디지털 라디오, 연결성(USB, HDMI, 블루투스)





이러한 예에서도 다른 모델, 제조업체 또는 위험 평가 간에 차이가 있을 수 있습니다. 예를 들어, 다른 요인에 따라 "엔진 관리" 위험은 ASIL C 또는 D가 될 수 있으며, 다양한 파워트레인 시스템과 위험은 ASIL B와 ASIL D 사이에서 다를 수 있습니다. 위험을 평가하고 수준을 할당하는 데는 많은 고려 사항이 있습니다.

또한 ASIL은 변경될 수 있습니다. 예를 들어, OEM(Original Equipment Manufacturer)은 구성 요소가 ASIL B 수준이라고 판단할 수 있지만 구성 요소가 다른 시스템과 통합되면 추가 위험 분석 및 위험 평가와 함께 수준을 높이거나 낮출 수 있습니다.

ASIL의 과제는 무엇입니까?

위의 차트는 심각도, 노출 및 제어 가능성 수준에 따라 ASIL에 도달하는 방법을 보여주지만, 이러한 수준을 할당하는 데는 어느 정도 주관성이 개입됩니다. 예를 들어, 도로 상태, 환경 요인, 교통 밀도, 운전자 역량 및 노출 가능성은 모두 크게 다를 수 있습니다. 넓고 비어 있고 건조한 도로에서 차량을 운전하는 운전자는 폭우 중에 교통량이 많은 곳에서 운전하는 운전자보다 위험한 사건을 제어할 가능성이 더 높을 수 있습니다. ASIL 분류 시스템은 "보통", "가능성이 있음", "아마도"와 같은 단어로 주관적인 해석에 따라 달라지며, 여기에는 엔지니어와 개발자의 어느 정도 수준의 교육적 판단이 포함됩니다. ASIL 수준을 결정하는 또 다른 과제는 전체 위험 분석 및 위험 평가를 수행하지 않고 과거 수준 할당을 기반으로 가정을 하는 유혹입니다. 예를 들어, 시스템에 이전에 ASIL 수준 B가 할당된 경우 현재 수준이 동일해야 한다고 가정하는 것이 유혹적일 수 있습니다. 그러나 시스템의 개선이나 다른 시스템과의 통합으로 수준이 변경될 수 있습니다. GPS 시스템이 이제 카메라 장비나 다른 지능형 기술과 통합된다면, 그 새로운 통합을 통해 ASIL 수준이 높아지거나 낮아질 수 있습니다.

마지막으로, 좋은 문서 기록을 유지하지 않거나 요구 사항을 제대로 추적하지 않는 팀은 부정확한 ASIL에 도달하거나 심지어 위험을 완전히 무시할 수도 있습니다. 문서와 요구 사항을 철저히 추적하지 않으면 팀은 주요 기능적 안전 위험을 놓칠 수 있습니다. 요구 사항 추적 및 추적성은 ISO 26262 준수뿐만 아니라 위험을 철저하고 정확하게 평가하고 완화해야 하는 실질적인 시장 요구에도 필수적입니다.

관련 기사: 자동차 Spice(ASPICE) 기능을 가속화하기 위한 모범 사례

ASIL은 제품 개발에 어떤 영향을 미칩니까?

시스템의 ASIL이 개발되면 ISO 26262는 ASIL에 따라 필요한 다양한 수준의 엄격성을 정의했습니다. 예를 들어, ASIL A 및 B의 경우 정보 표기법으로 요구 사항을 포착하기에 충분합니다. 이는 일반적으로 요구 사항이 자연어로 작성되고 간단한 그림으로 보강되어 주요 개념을 이해하지 못한다는 것을 의미합니다. ASIL C 및 D의 경우 보다 반공식적인 표기법이 권장됩니다. 요구 사항은 여전히 자연어로 작성되는 경우가 많지만 시스템 모델을 개발하여 동작을 보다 정확하게 설명합니다. 이러한 모델을 개발하려면 팀에 추가 전문 지식이 필요하지만 문서의 정확성이 높아지고 오해의 위험이 줄어듭니다. 더 높은 ASIL 시스템을 개발하는 팀은 프로세스를 지원하기 위한 추가 전문 지식과 특수 소프트웨어 도구가 필요한 경우가 많습니다.

ASIL은 어떻게 발전하고 있나요?

자동차 기술자 협회(SAE)는 심각도, 노출 및 제어 가능성을 평가하기 위한 추가 지침을 제공하기 위해 2015년에 J2980을 발행했습니다. 또한 J2980 자체는 ISO 26262와 마찬가지로 2018년에 업데이트되었습니다.

자동차 기술이 AI(인공지능), 자율 주행 기능, IoT(사물 인터넷)를 통한 외부 시스템과의 통합으로 발전함에 따라 제어 가능성의 개념은 특별한 과제를 안겨줍니다. 현재 "제어 가능성"은 주로 인간 차량 운전자를 의미하지만 자동차가 독립적으로 반응할 수 있는 능력이 커짐에 따라 제어 가능성을 평가하는 기준이 바뀔 수 있습니다. 운전자의 실수를 점점 더 많이 보상하는 기능을 통해 자동차는 더욱 안전하고 지능화되어 심각한 부상이나 사망을 초래하는 위험의 가능성이 줄어듭니다. 그러나 동시에 외부 시스템에 대한 액세스로 인해 ASIL 고려 사항을 복잡하게 만드는 사이버 취약성이 발생할 수 있습니다.

사이버 보안 취약성은 하드웨어 오류와 마찬가지로 안전 고려 사항으로 이어질 수 있습니다. 그 결과, 팀은 이제 시스템의 안전과 보안을 함께 분석하기 시작했습니다. ISO 21434는 특히 이 프로세스를 지원하기 위해 ISO 26262와 연계되는 권장 사항을 제시합니다.